IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

COALITION FOR INDEPENDENT TECHNOLOGY RESEARCH, *Plaintiff*,	§	
v.	§	No. 1:23-cv-00783
GREG ABBOTT, in his official capacity as Governor of the State of Texas, STEVEN C. MCCRAW, in his official capacity as Director and Colonel of the Texas Department of Public Safety, AMANDA CRAWFORD, in her official capacity as Executive Director of the Texas Department of Information Resources and Chief Information Officer of Texas, DALE RICHARDSON, in his official capacity as Chief Operations Officer of the Texas Department of Information Resources, ASHOK MAGO, LAURA WRIGHT, LINDY RYDMAN, CARLOS MUNGUIA, MARY DENNY, MILTON B. LEE, MELISA DENIS, DANIEL FEEHAN, and JOHN SCOTT, JR., in their official capacities as members of the Board of Regents of the University of North Texas System, and MICHAEL WILLIAMS, in his official capacity as Chancellor of the University of North Texas System, *Defendants*.	§	

DEFENDANTS' OPPOSITION TO PLAINTIFF'S MOTION FOR A PRELIMINARY INJUNCTION

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

GRANT DORFMAN
Deputy First Assistant Attorney General

JAMES LLOYD
Deputy Attorney General for Civil Litigation

KIMBERLY GDULA
Acting Division Chief, General Litigation Division

TODD A. DICKERSON
Attorney-in-Charge
Assistant Attorney General
Texas Bar No. 24118368
General Litigation Division
P.O. Box 12548, Capitol Station
Austin, Texas 78711-2548
(512) 463-2120 | FAX: (512) 320-0667
Todd.Dickerson@oag.texas.gov

COUNSEL FOR DEFENDANTS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

INTRODUCTION

The United States government (both the Biden and Trump Administrations), 36 states, and 14 countries have banned TikTok on government devices due to it being a national security threat. One of the main concerns is that the Chinese Communist Party ("CCP") can exploit its deep ties to TikTok to access the extensive data this social media platform collects on its users. This is not mere speculation. Chinese law *requires* TikTok to hand over this sensitive information upon request. And TikTok, through its parent company ByteDance, has used this data to spy on U.S. journalists in the past. Put simply, there are good reasons other states and governments around the world are limiting access to TikTok.

Coalition for Independent Technology Research sued Texas over its partial TikTok ban, which restricts access to TikTok on state-issued devices and personal devices authorized to use state information networks. Coalition argues that Texas's partial ban violates the First Amendment, even though this ban is practically indistinguishable from those passed by many other state and foreign governments. Coalition's claims are baseless, and no U.S. court has ever invalidated a partial TikTok ban such as Texas's.

This Court should deny Coalition's motion for a preliminary injunction. To begin, Coalition did not assert viable First Amendment claims, so it will not succeed on the merits. Texas's partial ban reaches only nonpublic forums (state-owned devices and networks), so it need only be "reasonable" to be constitutional. Texas's ban easily meets this light standard as it: (1) tracks the restrictions imposed by other states and countries; (2) plugs a vulnerability in state agencies' systems and networks; (3) focuses on a company with troubling ties to a foreign adversary; and (4) leaves open ample alternative methods for expression. Coalition also has justiciability challenges, as Defendants will explain below.

The other preliminary injunction factors also favor Defendants. The harm to Coalition's members is minimal—Coalition identified only one member whose scholarship is allegedly limited by

Texas's partial ban, and even this one member admits that she can still access TikTok. Further, the harm to Texas if the ban is lifted is significant; it would open a vulnerability in Texas's network that could be exploited by CCP-sponsored hackers.

Finally, this Court has held that an unjustified five-month delay in seeking emergency relief weighs against issuing a preliminary injunction. Coalition waited nine months after Texas first implemented its partial ban to file its motion for a preliminary injunction. It has not established, and cannot establish, good cause for waiting so long to seek an injunction. This Court should deny Coalition's motion for a preliminary injunction in its entirety.

BACKGROUND

I. TikTok Is a Unique Threat to the United States' Security Interests.

A. TikTok Has Deep Ties to the Chinese Government.

It is no secret that the CCP looms large over *any* Chinese-based company, and it has exploited its authority over Chinese tech companies in the past.[1] The CCP has the capacity to exert state power over TikTok through its corporate structure. TikTok is owned by ByteDance, a Chinese-based company.[2] ByteDance's executives are "heavily involved in TikTok's decision-making," so much so that the two companies' boundaries are "almost non-existent."[3] ByteDance, in turn, has deep ties to the Chinese government. For instance, one former ByteDance executive reported that the CCP has a "superuser credential" at ByteDance, giving it access to "all data collected by ByteDance including those of U.S. users."[4] And Forbes found that 300 ByteDance employees "previously worked for

[1] Lingling Wei, *China's New Way to Control Its Biggest Companies: Golden Shares*, WALL ST. J. (Mar. 8, 2023), https://tinyurl.com/587yf2e8.
[2] Sapna Maheshwari et al., *Bans on TikTok Gain Momentum in Washington and States*, N.Y. TIMES (Dec. 20, 2022), http://tinyurl.com/2nyv8nxt.
[3] Salvador Rodriguez, *TikTok Insiders Say Social Media Company is Tightly Controlled by Chinese Parent ByteDance*, CNBC (June 25, 2021), http://tinyurl.com/53rcytbf.
[4] *Former Exec at TikTok's Parent Company Says Communist Party Members had a 'God Credential' that let them Access Americans' Data*, BUS. INSIDER (June 7, 2023), http://tinyurl.com/3pywsfbb.

Chinese state media publications."[5]

B. The CCP Has Tremendous Power Over Chinese-Based Companies, and It Can Wield that Power to Devastating Effect.

The "Douyin" and "Jack Ma" incidents highlight the CCP's broad power over Chinese companies. In 2021, the Chinese government took a 1% stake in Douyin, which is China's version of TikTok run by another ByteDance subsidiary.[6] This is known as a "golden share," a nominal interest that "allow[s] government officials to be directly involved in [the business]."[7] Through this 1% interest, the Chinese government controlled *one-third* of the subsidiary's board seats, meaning the CCP could exert influence well beyond its small equity stake.[8]

The Chinese government can devastate even its richest private citizens. Take Jack Ma, the founder of the wildly successful tech company Alibaba. Ma lightly criticized Chinese regulations during a speech in October 2021.[9] He was "summoned by Chinese authorities for questioning" a week later.[10] The day after that, the Chinese government nixed a record-breaking IPO for one of Ma's companies, despite approving it earlier.[11] Ma disappeared from public life for years after this incident, and his fortune has since been cut in half.[12] Following two years of "hefty fines and sanctions," the CCP took

---

[5] Emily Baker-White, *Exclusive: TikTok Spied on Forbes Journalists*, FORBES (Dec. 22, 2022), http://tinyurl.com/y426c6p8.
[6] Jeanne Whalen, *Chinese Government Acquires Stake in Domestic Unit of TikTok Owner ByteDance in Another Sign of Tech Crackdown*, WASH. POST (Aug. 17, 2021), http://tinyurl.com/yf233pbw.
[7] Laura He, *China Still Wants to Control Big Tech, It's Just Pulling Different Strings*, CNN (Jan. 27, 2023), http://tinyurl.com/3ab2r23n.
[8] Whalen, *supra* note 6.
[9] Charlie Campbell, *Where is Alibaba Founder Jack Ma? What the Saga of One of the World's Richest Men Reveals About China Under Xi Jinping*, TIME (Jan. 4, 2021), http://tinyurl.com/4jv7cjz3.
[10] *Id.*
[11] *Id.*
[12] Michelle Toh, *Jack Ma Loses More than Half of His Wealth After Criticizing Chinese Regulators*, CNN (July 12, 2023), http://tinyurl.com/2p4zjcb7; *Jack Ma Isn't Back*, WIRED (June 15, 2023), http://tinyurl.com/2p9w7txk; Mark Sweney, *Alibaba Founder Jack Ma Hiding Out in Tokyo, Reports Say*, GUARDIAN (Nov. 29, 2022), http://tinyurl.com/5cbccw3r.

its "golden share" of Alibaba.[13] Ma ceded control of the company soon after.[14]

C. The Chinese Government Codified its Power to Access TikTok's User Data and that of Other Private Companies.

In 2017, the CCP implemented a law that "requires companies to give the government any personal data relevant to the country's national security."[15] As FBI Director Christopher Wray explained, this law forces Chinese companies "to do whatever the government wants them to do in terms of showing them information or serving as a tool for the Chinese government."[16]

This means the extensive data TikTok collects on its users is at the CCP's fingertips. This includes: (1) messages the user sends on TikTok; (2) user credit card information; (3) the user's phone and social network contacts; (4) what videos the user watches; (5) the user's search history; (6) the user's "keystroke patterns or rhythms"; and (7) the user's location.[17]

D. ByteDance Covertly Tracked U.S. Reporters Using TikTok, and TikTok May Be Using Malicious Software to Collect User Data.

In late 2022, Forbes published a series of articles exposing TikTok's ties to the CCP.[18] ByteDance responded by secretly tracking Forbes journalists' user data from TikTok to unearth the source of the leaks.[19] ByteDance later admitted "that its employees had inappropriately obtained the

---

[13] Mark Sweney, *China to Take 'Golden Shares' in Tech Firms Alibaba and Tencent*, GUARDIAN (Jan. 13, 2023), http://tinyurl.com/58zx37su.
[14] *Id.*
[15] *The TikTok Wars—Why the US and China are Feuding Over the App*, GUARDIAN (Mar. 16, 2023), http://tinyurl.com/2a8kejuz.
[16] *TikTok: Why do Countries Think Chinese Tech Firms are a Security Risk?*, BBC (Mar. 24, 2023), http://tinyurl.com/crreue7w.
[17] *Privacy Policy*, TIKTOK (last updated May 22, 2023), http://tinyurl.com/27rbp89v.
[18] *See* Emily Baker-White, *A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns*, FORBES (Oct. 25, 2022), http://tinyurl.com/5n7ty5vp; Emily Baker-White, *TikTok is Bleeding U.S. Execs Because China is Still Calling the Shots, Ex-Employees Say*, FORBES (Sept. 21, 2022), http://tinyurl.com/eyj5azef; Emily Baker-White, *LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State Media—and Some Still Do*, FORBES (Aug. 11, 2022), http://tinyurl.com/5c6tnump.
[19] *Exclusive: TikTok Spied on Forbes Journalists*, *supra* note 5; Cecilia Kang, *ByteDance Inquiry Finds Employees Obtained User Data of 2 Journalists*, N.Y. TIMES (Dec. 22, 2022), http://tinyurl.com/r3bk3btw.

data" of the American users in question.[20] Nothing stops the Chinese government from doing the same tracking, or more, by exploiting its access to TikTok.

In fact, recent media reports indicate that "[t]he web browser used within the TikTok app can track every keystroke made by its users."[21] This practice, also known as "keylogging," is often used by hackers to "intercept a victim's usernames, passwords, and other sensitive information."[22] According to the New York Times, it is "not common" for a major commercial application to contain this invasive function.[23]

Let that sink in. It's possible that, through the Trojan horse of an addictive social media platform, the CCP has effectively tricked over 100 million Americans into downloading malicious hacking software that can be used to invade their most intimate secrets and ruin their lives.

E. The "Pegasus" Problem.

Spyware has gotten exponentially more sophisticated, invasive, and difficult to detect in the last decade. Explaining the threat high-level cyberattacks pose helps show why TikTok is a serious security risk.

Consider the software "Pegasus," which is one of the most powerful hacking tools ever

---

[20] Glenn Thrush and Sapna Maheshwari, *Justice Dept. Investigating TikTok's Owner Over Possible Spying on Journalists*, N.Y. TIMES (Mar. 17, 2023), http://tinyurl.com/3wa3rayn.

[21] *See, e.g.*, Paul Mozur et al., *TikTok Browser Can Track Users' Keystrokes, According to New Research*, N.Y. TIMES (Aug. 19, 2022), http://tinyurl.com/2bfyv7rh.

[22] Danielle Drora Greenstein, *A Landlord's Obligation to Protect the Sensitive Information of Potential and Current Lessees' from Identity Theft*, 28 U. FLA. J.L. & PUB. POL'Y 519, 523 (2017); *Spying with Technology*, 2020 TXCLE-AFL 34-III, 2020 WL 5608154 ("Keystroke logger spyware is a malicious program used by hackers. This program is designed to steal personal information by logging the actual keystrokes you type on your computer. When you enter a PIN, password, or credit card number the keyword logger records it for the hacker.").

[23] Paul Mozur et al., *supra* note 21.

developed.[24] Pegasus can infect a phone without any interaction from the phone's owner.[25] A hacker can use Pegasus to send malware merely by placing a call to an individual, even if the target doesn't answer.[26] This is what happened in 2019, when hackers used Pegasus to install malware on over 1,000 phones merely by placing calls to target devices through WhatsApp.[27] Pegasus was also used to exploit vulnerabilities in Apple's iMessage software to gain access to hundreds of millions of iPhones.[28]

Once inside a device, Pegasus's access is total. It can harvest any information on that phone and monitor everything the user does on it in real time.[29] This includes watching through a phone's camera and listening through its microphone, even while the phone appears to be off.[30] Pegasus gives a hacker "root privileges" to a phone, which means the hacker effectively has more control over the phone than its user does.[31] Pegasus is designed to inhabit only a phone's temporary memory, which means there are virtually no traces of the software once the phone is powered down.[32]

Pegasus worms its way into users' devices by exploiting flaws in an operating system or software that the manufacturer is unaware of.[33] Yet the CCP would not have to sift through the code of popular applications for undiscovered vulnerabilities. If truly in control, the CCP could *create*

---

[24] David Pegg and Sam Cutler, *What is Pegasus Spyware and how does it Hack Phones*, GUARDIAN (July 18, 2021), https://tinyurl.com/5y7tvt9n.
[25] *Id.*; Mark Mazzetti et al., *How the Global Spyware Industry Spiraled Out of Control*, N.Y. TIMES (Jan. 28, 2023), https://tinyurl.com/3m4xanrk.
[26] David Pegg and Sam Cutler, *supra* note 24.
[27] *Id.*
[28] *Id.*
[29] *Id.*; Natalie Kitroeff and Ronen Bergman, *How Mexico Became the Biggest User of the World's Most Notorious Spy Tool*, N.Y. TIMES (Apr. 18, 2023), https://tinyurl.com/35fday52.
[30] Natalie Kitroeff and Ronen Bergman, *supra* note 29; Ronen Bergman and Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y TIMES MAGAZINE (Jan. 28, 2022), https://tinyurl.com/bcrwyvde.
[31] David Pegg and Sam Cutler, *supra* note 24.
[32] *Id.*
[33] *Id.*

difficult-to-detect vulnerabilities in TikTok and access everything on the TikTok-installed device.[34]

Secret backdoors aside, TikTok is still an immensely powerful tool for the CCP. Like many popular social media applications, TikTok's terms of service requires users to grant access to a device's camera and microphone.[35] The CCP could easily exploit this granted access to eavesdrop on TikTok users' conversations.[36]

F. Numerous States and Countries Restrict Access to TikTok.

Given the issues above, it should be no surprise that states and governments across the world are starting to restrict access to TikTok. Both the Biden and Trump Administrations banned TikTok on government devices due to national security concerns,[37] and 36 states in this country have similarly restricted TikTok.[38] As Representative Raja Krishnamoorthi explained, there is "widespread concern [about TikTok] at this point—it's not just Republicans, it's not just Democrats."[39]

Looking beyond our nation's borders, each of the "five eyes" intelligence-sharing partners—U.S., Canada, Britain, New Zealand, and Australia—banned TikTok on governmental devices within

---

[34] *See Five Ways TikTok is Seen as Threat to US National Security*, SECURITY WEEK (Dec. 22, 2022) ("'Maybe with TikTok we are just clicking and installing the Chinese version of Pegasus on our devices. I think that is the worry of the US government'") (quoting Etay Maor, senior director of security strategy at Cato Networks) (ellipses omitted), https://tinyurl.com/mptej4bb.

[35] Emil Sayegh, *TikTok Users are Bleeding Data*, FORBES (Nov. 9, 2022), https://tinyurl.com/yck3y6ek; *see also Privacy Policy*, *supra* note 17 (stating that TikTok collects information on its users' "connected audio devices"); Declaration of Meghan Frkuska ("Frkuska Decl."), ¶ 5.

[36] Emil Sayegh, *supra* note 35; Frkuska Decl., ¶ 5.

[37] Executive Order 13942, 85 FR 48637 (Aug. 6, 2020); *Feb. 27, 2023 Memorandum for the Heads of Executive Departments and Agencies*, OFF. MGMT. & BUDGET (the "*February 27th Memorandum*"), *available at* http://tinyurl.com/4mw7s48e.

[38] Andrew Adams, *Updated: Where is TikTok Banned? Tracking State by State*, GOV'T TECH. (last updated Apr. 6, 2023), https://tinyurl.com/bdfu46tf.

[39] *Bans on TikTok Gain Momentum in Washington and States*, *supra* note 2.

weeks of each other.[40] So too did Belgium,[41] Denmark,[42] Estonia,[43] the European Union,[44] India,[45] Latvia,[46] Netherlands,[47] Norway,[48] and Taiwan.[49]

Texas is not jumping at its shadow. TikTok is a worldwide danger for reasons well beyond it being an addictive social media application.[50] It is alarming that the countries noted above—backed by some of the best intelligence agencies on the planet—all agree on this point.

II. An Overview of Texas's Partial TikTok Ban.

In December 2022, Governor Abbott banned the use of TikTok on state-issued devices.[51] In this Directive, he explained that news media reports had exposed TikTok's close ties to the CCP and revealed that this application was a threat to Texas's "sensitive information and critical infrastructure."[52] Governor Abbott also instructed the Department of Information Resources ("DIR") and the Department of Public Safety ("DPS") "to develop a model plan that other state

---

[40] *Which Countries have Banned TikTok and Why?*, EURONEWS (Apr. 4, 2023), http://tinyurl.com/2fwa732h.
[41] *Belgium Bans TikTok from Government Phones After US, EU*, APNEWS (Mar. 10, 2023), http://tinyurl.com/mrxr832k.
[42] *Id.*
[43] *Minister Jarvan: TikTok to be Banned on State Officials' Work Phones*, ERR (Mar. 29, 2023), http://tinyurl.com/yc2ucfnj.
[44] Alex Hern, *Canada Bans TikTok on Government Devices over Security Risks*, GUARDIAN (Feb. 28, 2023), http://tinyurl.com/r35kp6fn.
[45] Sapna Maheshwari and Amanda Holpuch, *Why Countries are Trying to Ban TikTok*, N.Y. TIMES (Aug. 16, 2023), http://tinyurl.com/3uad5h58.
[46] Kelvin Chan, *Here are the Countries that have Bans on TikTok*, APNEWS (Apr. 4, 2023), http://tinyurl.com/5hybrh3w.
[47] Mike Corder, *Dutch Gov't Staff Discouraged from Apps such as TikTok*, APNEWS (Mar. 21, 2023), http://tinyurl.com/ms65d4k2.
[48] *China Criticizes Possible US Plan to Force TikTok Sale*, APNEWS (Mar. 23, 2023), http://tinyurl.com/yc8knfdv.
[49] *TikTok Banned on U.S. Government Devices, and the U.S. is Not Alone. Here's Where the App is Restricted*, CBSNEWS (Mar. 1, 2023), http://tinyurl.com/3c3jux3j.
[50] *See, e.g.*, Julie Jargon, *TikTok Feeds Teens a Diet of Darkness*, WALL ST. J. (May 13, 2023), https://tinyurl.com/ee3wmcuz; Julie Jargon, *TikTok Brain Explained: Why Some Kids Seem Hooked on Social Video Feeds*, WALL ST. J. (Apr. 2, 2022), https://tinyurl.com/2w52cr2w.
[51] ECF 1-2, 2.
[52] *Id.*

agencies can deploy" covering whether the ban should extend to personal devices.[53]

DIR and DPS issued the Model Plan in January 2023.[54] The plan proposed that the TikTok ban should extend to personal devices used "to conduct state business."[55] The plan defined "state business" to "include[] accessing any state-owned data, applications, email accounts, or non-public facing communications."[56]

The Texas Legislature recently passed SB 1893, which codified most of the Directive.[57] Under SB 1893, government entities must adopt a policy "prohibiting the installation or use of [TikTok] on any device owned or leased by the governmental entity and requiring the removal of covered applications from these devices."[58] Taken together, state employees are barred from accessing TikTok on (1) state-issued devices and (2) personal devices used to connect to state networks. The Directive, Model Plan, and SB 1893 contemplate that state agencies are responsible for banning TikTok at their respective agencies.[59] This tracks Tex. Admin. Code § 202.20(a), which states: "The agency head of each state agency is ultimately responsible for the agency's information resources." Tex. Admin. Code § 202.70(a) similarly provides: "The agency head of each state institution of higher education is ultimately responsible for the security of state information resources."

---

[53] *Id.* at 3.
[54] ECF 1-3.
[55] *Id.* at 6.
[56] *Id.*
[57] Tex. Gov't Code §§ 620.001 *et seq.*
[58] *Id.* at § 620.003(a); *see also id.* at § 620.001(1).
[59] *See* ECF 1-2, 3 (stating that the TikTok ban on state-issued devices "must be strictly enforced by your agency IT department" and that the agency head has nondelegable authority to grant exceptions to this ban); ECF 1-3, 4 ("Each agency is responsible for the implementation of the plan as outlined in this document, including any changes to meet specific agency needs."); *id.* at 8 ("It is the responsibility of each agency to implement the removal and prohibition of any offending technology."); *id.* at 9 ("Each agency is required to develop its own security policy to support the implementation of this plan."); Tex. Gov't Code § 620.003(a) ("[A] governmental entity shall adopt a policy prohibiting the installation or use of a covered application on any device owned or leased by the governmental entity and requiring the removal of covered applications from these devices.").

III. An Overview of Coalition's Complaint and the Procedural History.

Coalition claims that Texas's partial TikTok ban violates the First Amendment as applied to public university faculty.[60] Coalition alleges that one of its members, University of North Texas System ("UNT") professor Jacqueline Vickery, wants to conduct research and teach about TikTok.[61] Yet it did not dispute that Professor Vickery can access TikTok on her personal device, so long as that device was not used to connect to UNT's network. Nor did Coalition meaningfully distinguish Texas's partial TikTok ban from those adopted by many other states and countries.

On September 7, 2023, Coalition filed a motion for a preliminary injunction.[62] This motion came nine months after Governor Abbott's Directive partially banning TikTok.[63] On September 8, 2023, Defendants filed a motion to dismiss under Rule 12(b)(1) and 12(b)(6), raising many of the same arguments asserted here.[64]

STANDARD OF REVIEW

To obtain a preliminary injunction, the moving party must show: "(1) a substantial likelihood of success on the merits, (2) a substantial threat of irreparable harm if the injunction does not issue, (3) that the threatened injury outweighs any harm that will result if the injunction is granted, and (4) that granting the injunction is in the public interest."[65] The purpose of a preliminary injunction "is to maintain the status quo until the parties have the chance to adjudicate the merits."[66] Such an injunction

[60] ECF 1, pg. 23 (Prayer for Relief).
[61] *See id.* at ¶¶ 46–47.
[62] ECF 20.
[63] *See* ECF 1, ¶¶ 34–35; ECF 1-2; ECF 20-2, ¶ 46
[64] *See* ECF 21.
[65] *Clarke v. Commodity Futures Trading Comm'n*, 74 F.4th 627, 640–41 (5th Cir. 2023).
[66] *Feds for Med. Freedom v. Biden*, 63 F.4th 366, 389 (5th Cir. 2023); *see also Martinez v. Mathews*, 544 F.2d 1233, 1243 (5th Cir. 1976) ("Mandatory preliminary relief, which goes well beyond simply maintaining the status quo pendente lite, is particularly disfavored, and should not be issued unless the facts and law clearly favor the moving party.") (citation omitted).

is an "extraordinary" and "drastic" remedy that is "not to be granted routinely."[67]

ARGUMENT

I. Coalition is Not Likely to Succeed on the Merits.

A. Most of Coalition's Claims are Nonjusticiable.

1. An Overview of *Ex parte Young* and Article III Standing.

State entities and officials are generally entitled to sovereign immunity unless an exception applies.[68] Coalition relies on the *Ex parte Young* exception here. This exception requires the defendant being sued to have "a sufficiently close connection to the unlawful conduct."[69] This means that the state official must have "the particular duty to enforce" the statute or policy in question and a "demonstrated willingness to exercise that duty."[70]

For Article III standing, the plaintiff must show that it suffered: (1) an injury in fact; (2) that is fairly traceable to the defendants' actions; (3) that is likely to be redressed by a favorable outcome.[71] "[A] plaintiff must demonstrate standing for each claim he seeks to press and for each form of relief that is sought."[72] The standing and *Ex parte Young* analyses "significant[ly] overlap."[73]

2. Coalition's Only Justiciable Claims are Those Against Chancellor Williams.

The justiciability issues here are best understood through *Ex parte Young's* "enforcement" requirement, although the same general arguments apply to Article III's traceability prong.

Chancellor Williams is a proper enforcement officer. The Directive, Model Plan, SB 1893, and Tex. Admin. Code § 202.70(a) all contemplate that each agency, or the "agency head," is responsible

[67] *White v. Carlucci*, 862 F.2d 1209, 1211 (5th Cir. 1989).
[68] *Lewis v. Scott*, 28 F.4th 659, 663 (5th Cir. 2022).
[69] *Freedom From Religion Found., Inc. v. Mack*, 4 F.4th 306, 311–12 (5th Cir. 2021).
[70] *Morris v. Livingston*, 739 F.3d 740, 746 (5th Cir. 2014) (quotations omitted).
[71] *Abdullah v. Paxton*, 65 F.4th 204, 208 (5th Cir. 2023).
[72] *Davis v. Fed. Election Comm'n*, 554 U.S. 724, 734 (2008) (quotations omitted).
[73] *Air Evac EMS, Inc. v. Tex., Dep't of Ins., Div. of Workers' Comp.*, 851 F.3d 507, 513–14 (5th Cir. 2017).

for enforcing the partial TikTok ban at their respective agencies.[74] Thus, Defendants do not dispute that Chancellor Williams is a proper party to this lawsuit.

But Coalition did not establish an enforcement connection for the other Defendants. "Where a state actor or agency is statutorily tasked with enforcing the challenged law and a different official is the named defendant, our *Young* analysis ends."[75] This principle bars the claims against all Defendants except Chancellor Williams and UNT's Board of Regents.[76] In short, Coalition's claims against Governor Abbott, DPS Director McCraw, DIR Director Crawford, and DIR Chief Operations Officer Richardson are nonjusticiable as these are not the identified officials responsible for enforcing the partial TikTok ban at Texas public universities.

Coalition's claims against UNT's Board of Regents fail for slightly different reasons. Coalition sued UNT's Board because "the UNT System Administration prohibited all UNT employees from using TikTok on state-issued or -managed devices."[77] Coalition missed that UNT's Board of Regents Rules "delegate authority to the Chancellor to develop and adopt System policies" such as this.[78] Put simply, UNT's Board was not involved in UNT's implementation of the partial TikTok ban, and Coalition presented no facts suggesting otherwise.

Finally, Defendants' alleged role in enacting the disputed policies does not make them enforcement officers under *Ex parte Young*. The Fifth Circuit has been clear on this point: "formulating

---

[74] *Supra*, 8–9.
[75] *City of Austin v. Paxton*, 943 F.3d 993, 998 (5th Cir. 2019).
[76] The UNT Board of Regents Defendants are Ashok Mago, Laura Wright, Lindy Rydman, Carlos Munguia, Mary Denny, Milton B. Lee, Melisa Denis, Daniel Feehan, and John Scott Jr.
[77] ECF 1, ¶ 13.
[78] *See* UNT Board of Board of Regents Rule § 2.201; *see also* UNT Board of Regents Rule § 4.101 ("The Chancellor heads the System Administration, which is used by the Board to exercise its powers and authorities in the governance of the System."). Copies of these rules are attached as Exhibits 1–2. They are publicly available at the following website: http://tinyurl.com/2zm5zf3c.

and promulgating the [disputed] policy does not subject [the official] to suit under *Ex parte Young*."[79]

3. Coalition's Claims Are Limited to UNT Due to Justiciability Issues.

While Coalition challenges Texas's ban "as applied to public university faculty,"[80] it lacks standing to assert a claim against Texas universities other than UNT. First, Coalition did not sue officials from any universities other than UNT. As explained above, this would be needed to establish *Ex parte Young's* "enforcement connection" requirement and for traceability reasons. Second, Coalition relies on associational standing, as it did not assert an organizational injury.[81] Yet Coalition cannot claim associational standing to sue Texas universities other than UNT because it did not allege that it has members at these other colleges.[82] Finally, a party generally cannot "challenge a statute as-applied unless the statute has been applied to him."[83] Coalition cannot contest other schools' bans as it did not allege that these bans were ever "applied" to any of its members.

For the justiciability reasons above, this Court should find that Coalition's claims are limited to UNT.

B. Coalition did Not Assert Viable First Amendment Claims.

Coalition's First Amendment claims fail on the merits. Here, the relevant government property—UNT's devices and networks—are nonpublic forums, which trigger lighter constitutional

---

[79] *Haverkamp v. Linthicum*, 6 F.4th 662, 670 (5th Cir. 2021); *Mi Familia Vota v. Abbott*, 977 F.3d 461, 467–68 (5th Cir. 2020) (finding that Governor Abbott was not the enforcement officer for his executive orders as the "statutory authority . . . to issue, amend or rescind an Executive Order is not the power to enforce it") (quotations omitted).

[80] ECF 1, pg. 23 (Prayer for Relief).

[81] *See id.* at ¶¶ 46–50; *cf. OCA-Greater Houston v. Texas*, 867 F.3d 604, 610 (5th Cir. 2017); *NAACP. v. City of Kyle*, 626 F.3d 233, 238 (5th Cir. 2010).

[82] *See Ass'n of Am. Physicians & Surgeons, Inc. v. Tex. Med. Bd.*, 627 F.3d 547, 550 (5th Cir. 2010) (explaining that, to have associational standing, the plaintiff must show that "its members would . . . have standing to sue in their own right").

[83] *Ctr. for Individual Freedom v. Carmouche*, 449 F.3d 655, 659 (5th Cir. 2006); *see also Davis v. Scherer*, 468 U.S. 183, 189 (1984) ("As the current state statute was never applied to appellee, he lacks standing to question its constitutionality.").

scrutiny. Texas's partial TikTok ban easily survives this lenient test. In fact, due to the nature of the problem and the ban's limited scope, Texas's ban would be constitutional under even the more rigorous scrutiny applied to designated and traditional public forums.

1. The Forum Analysis Applies Here, and an Overview of this Analysis.

First Amendment rights are more limited in the context of government-owned property. "Where the government is acting as a proprietor, managing its internal operations, . . . its action will not be subjected to the heightened review to which its actions as a lawmaker may be subject."[84] The Supreme Court devised a "forum analysis" to review First Amendment restrictions on government property.[85] This analysis applies here as Texas's partial ban extends only to state-owned property, such as state-issued laptops and personal devices used to access state networks.[86]

Courts generally "recognize three types of government-controlled spaces: traditional public forums, designated public forums, and nonpublic forums."[87] "Traditional public forums are places that by long tradition or by government fiat have been devoted to assembly or debate."[88] Designated public forums are "spaces that have not traditionally been regarded as a public forum but which the government has intentionally opened up for that purpose."[89] Nonpublic forums are spaces that "[are] not by tradition or designation a forum for public communication."[90]

The level of scrutiny turns on the type of forum involved. In traditional and designated forums,

---

[84] *Int'l Soc. for Krishna Consciousness, Inc. v. Lee*, 505 U.S. 672, 678 (1992).
[85] *Minn. Voters All. v. Mansky*, 138 S. Ct. 1876, 1885 (2018).
[86] The analysis would be different if Texas fully banned TikTok, like the Montana legislature recently did. *See* Sapna Maheshwari, *Montana Governor Signs Total Ban of TikTok in the State*, N.Y. TIMES (May 17, 2023), http://tinyurl.com/47rx3fs8; *Globe Newspaper Co. v. Superior Court for Norfolk Cnty.*, 457 U.S. 596, 607 n.17 (1982).
[87] *Mansky*, 138 S. Ct. at 1885.
[88] *Chiu v. Plano Indep. Sch. Dist.*, 260 F.3d 330, 344 (5th Cir. 2001) (quotations omitted).
[89] *Mansky*, 138 S. Ct. at 1885 (quotations omitted).
[90] *Id.* (quotations omitted). Some courts call nonpublic forums "limited public forum[s]." *See NAACP v. City of Philadelphia*, 834 F.3d 435, 441 (3d Cir. 2016); *see also Freedom From Religion Found. v. Abbott*, 955 F.3d 417, 426 (5th Cir. 2020).

"the government may impose reasonable time, place, and manner restrictions on private speech, but restrictions based on content must satisfy strict scrutiny, and those based on viewpoint are prohibited."[91] Yet the government "has much more flexibility" to limit speech in nonpublic forums.[92] There, "[t]he government may reserve such a forum for its intended purposes, communicative or otherwise, as long as the regulation on speech is reasonable and not an effort to suppress expression merely because public officials oppose the speaker's view."[93]

2. UNT's IT Resources are Nonpublic Forums.

When defining the forum, the focus is "on the access sought by the speaker."[94] Coalition alleges that UNT professor Vickery cannot use her "university-owned laptop" or her "university-owned on-campus desktop" to access TikTok on "university-managed internet networks."[95] And it alleges that Professor Vickery cannot use TikTok on her personal cellphone because she "also uses it to access" UNT services such as her "university email" and "university Zoom account."[96] All these devices fall under the umbrella of "IT resources."[97] Thus, we analyze whether UNT's IT resources are traditional, designated, or nonpublic forums.

UNT's IT resources are not traditional public forums. This category is limited to forums that "immemorially" have been held open for First Amendment purposes.[98] But government-issued

[91] *Mansky*, 138 S. Ct. at 1885.
[92] *Id.*
[93] *Id.* (quotations omitted).
[94] *Cornelius v. NAACP Legal Def. & Educ. Fund, Inc.*, 473 U.S. 788, 801–02 (1985).
[95] ECF 1, ¶¶ 46–49.
[96] *Id.* at ¶ 47. Professor Vickery alleges that it is "infeasible" for her to use her phone to perform scholarly research and that she "does not have a personal laptop or desktop." *Id.* Thus, she apparently was not harmed by the portion of the ban extending to personal devices. Even if she was, it does not meaningfully change the forum analysis here.
[97] *See* Ex. 3, 9 (defining "information resources" as "[t]he procedures, equipment, and software employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information and associated personnel including consultants and contractors.").
[98] *United States v. Am. Libr. Ass'n, Inc.*, 539 U.S. 194, 205–06 (2003); *see also Ark. Educ. Television Comm'n v. Forbes*, 523 U.S. 666, 678 (1998).

devices have *never* been thought of as fora for freewheeling public debate. Such devices are not open to the public at all—being instead a privilege given to university employees alone or individuals acting on behalf of the university in furtherance of government business. In any event, even government employees who do have access are given those tools to perform the work of the government, not to amplify their private views in a digital public square.

Thus, the question is whether UNT's IT resources are designated or nonpublic forums. As we will show, the restrictions UNT places on these resources, the fora's nature, and the relevant caselaw all support the conclusion that only a nonpublic forum is implicated here.

(a) UNT Heavily Regulates its IT Resources.

The government creates only a nonpublic forum when it requires individuals to "obtain permission" to access its property[99] or otherwise regulates use of that property.[100] Supreme Court caselaw "illustrate[s] the distinction between 'general access,' which indicates the property is a designated public forum, and 'selective access,' which indicates the property is a nonpublic forum."[101]

UNT heavily regulates its IT resources. Judicially noticeable documents, such as UNT's Information Security Handbook and its formal policies,[102] and other evidence[103] show that UNT:

- specifies that its "information resources are a non-public forum" by default;[104]

[99] *Ark. Educ. Television Comm'n*, 523 U.S. at 679–80.
[100] *Mansky*, 138 S. Ct. at 1886 (finding that a polling place was a nonpublic forum in part because "[r]ules strictly govern who may be present [at a polling place], for what purpose, and for how long").
[101] *Ark. Educ. Television Comm'n*, 523 U.S. at 679 (citations omitted).
[102] *See, e.g.*, *Kitty Hawk Aircargo, Inc. v. Chao*, 418 F.3d 453, 457 (5th Cir. 2005) (taking judicial notice of information posted on the National Mediation Board's website); *Coleman v. Dretke*, 409 F.3d 665, 667 (5th Cir. 2005) ("[W]e fail to see any merit to an objection to the panel taking judicial notice of the state agency's own website."); *O'Toole v. Northrop Grumman Corp.*, 499 F.3d 1218, 1225 (10th Cir. 2007) ("It is not uncommon for courts to take judicial notice of factual information found on the world wide web.").
[103] *See* Declaration of Richard Anderson ("Anderson Decl."), ¶¶ 8–10.
[104] Ex. 4, 2–3. This policy is publicly available at the following website: http://tinyurl.com/mff4p5un.

- allows only "authorized" users and networks to access its IT resources;[105]
- retains the "sole discretion" to "revoke authorization at any time" and to "limit the use of Information Resources to specific research, teaching missions or other purposes";[106]
- bars users from "sending spam messages," using its resources "for a personal commercial purpose," and taking various other acts;[107]
- prohibits the "introduction of network devices or information resources that negatively affect the behavior or security of the network or violate university policies";[108] and
- reserves the right to sanction users who violate its access and use policies.[109]

Thus, UNT restricts use of and access to its IT resources, which means the nonpublic forum analysis applies here.[110] Coalition offered no facts that would plausibly change this conclusion.

(b) The "Nature of the Government Property" Further Supports a Finding that UNT's IT Resources Are Nonpublic Forums.

In *Cornelius v. NAACP Legal Def. & Educ. Fund, Inc.*, the Supreme Court noted that forums at a government workplace are more likely to be considered nonpublic. The Court explained that "[t]he Government, as an employer, must have wide discretion and control over the management of its personnel and internal affairs."[111] This principle applies here. Coalition admits that UNT provides IT resources to professors like Vickery to facilitate their work for UNT.[112] The fact that UNT is largely acting in its capacity as an employer in this regard "strengthens the conclusion" that UNT's IT resources are nonpublic forums.[113]

Relevant caselaw shows that UNT's IT resources are nonpublic forums. In *United States v.*

---

[105] Ex. 3, 18 ("Access agreements must be established prior to granting employee and contractor access to institutional information and information resources."); *see also id.* at 24, 40; Anderson Decl., ¶¶ 9–10. UNT System's Information Security Handbook is publicly available at the following website: http://tinyurl.com/488rfn6v.
[106] Ex. 4, 3; Anderson Decl., ¶ 10.
[107] Ex. 4, 7–9.
[108] Ex. 3, 40.
[109] *Id.* at 64.
[110] *See, e.g.*, *Ark. Educ. Television Comm'n*, 523 U.S. at 679–80.
[111] *Cornelius*, 473 U.S. at 805 (quotations omitted).
[112] *See* ECF 1, ¶¶ 46–49.
[113] *See Cornelius*, 473 U.S. at 805.

American Library Association Inc., the Supreme Court found that a public library's system of computers furnishing internet access was a nonpublic forum. First, the forum under the microscope was not "the internet" writ large, but rather *the library-owned devices* capable of accessing the internet, which the library provided for patrons.[114] Second, the Court explained that a library does not furnish computers "to create a public forum for Web publishers to express themselves."[115] Rather, it does so "to facilitate research, learning, and recreational pursuits by furnishing materials of requisite and appropriate quality."[116] *American Library* shows that school-provided internet and other IT resources are best thought of as tools to facilitate a school's mission; they are not public forums open to free expression.

Indeed, courts have found the following to be nonpublic forums: a school's internal mail system (including email);[117] a prison's electronic system for communicating with inmates;[118] a college's electronic system for attending virtual classes and submitting assignments;[119] state computer internet terminals;[120] and university computer services.[121] This Court should follow all others and find that UNT's IT resources are nonpublic forums.

3. The Partial TikTok Ban is Reasonable in Light of the Forums' Purposes.

TikTok users undoubtedly may use the program to express a variety of views.[122] But Texas's partial ban makes no distinction based on users' viewpoints—or even based on viewpoints that

[114] *Am. Libr. Ass'n, Inc.*, 539 U.S. at 206.
[115] *Id.* at 206–07.
[116] *Id.*
[117] *Perry Educ. Ass'n v. Perry Local Educators' Ass'n*, 460 U.S. 37, 46–48 (1983); *Chiu*, 260 F.3d at 350; *Pichelmann v. Madsen*, 31 F. App'x. 322, 327 (7th Cir. 2002).
[118] *Witzke v. Bouchard*, No. 22-13070, 2023 WL 3919303, at *6 (E.D. Mich. June 9, 2023).
[119] *Collins v. Putt*, No. 3:17-CV-01621(AVC), 2019 WL 8501541, at *1, 4 (D. Conn. Mar. 28, 2019).
[120] *Nickolas v. Fletcher*, No. 3:06 CV 00043 KKC, 2007 WL 1035012, at *1, 5–6 (E.D. Ky. Mar. 30, 2007).
[121] *Loving v. Boren*, 956 F. Supp. 953, 954 (W.D. Okla. 1997).
[122] *See NetChoice, LLC v. Paxton*, 49 F.4th 439, 459–60 (5th Cir. 2022).

TikTok itself might convey on its platform.[123] Thus, the question is whether this ban is "reasonable in light of the purpose served by the forum[s]."[124] It clearly is.

UNT provides IT resources mainly "for the purpose of conducting University business."[125] While UNT allows some use of its IT resources for personal reasons, this is incidental to UNT's primary motive.[126] Indeed, UNT *must* provide these services to fulfill its mission of "advancing educational excellence and preparing students to become thoughtful, engaged citizens of the world."[127]

Other "purposes" logically include the need for privacy, the safety of its users, and the security of the system. UNT's IT resources would be useless if shut down by a cyberattack. And individuals would not utilize these resources if use carried a significant risk of being hacked.

The partial TikTok ban is reasonably related to these purposes. Again, the CCP has the power to, at any time, use its access to TikTok or its 2017 national security law to exploit users' location data, personal messages, passwords, and other sensitive data.[128] This ever-present threat carries obvious dangers. Stolen passwords could be used to gain access to UNT's network. Sensitive cyber-defense research could be funneled directly to the CCP. (After all, both the NSA and the Department of

---

[123] *See id.* at 462.
[124] *Cornelius*, 473 U.S. at 806.
[125] Ex. 4, 3.
[126] *See id.* ("University students may use University information resources for school- related and personal purposes in accordance with this policy and other applicable University policies, and state and federal law, provided personal use does not result in any additional costs to the University."); *id.* ("University employees and authorized individuals may use Information Resources in accordance with this policy and other applicable University policies . . . . Incidental personal use of Information Resources by employees and authorized individuals is permitted, subject to review and reasonable restrictions by the employee's supervisor, provided the use does not interfere with the performance of job responsibilities and does not result in any additional costs to the University."); *id.* ("The University may limit the use of Information Resources to specific research, teaching missions or other purposes at its sole discretion . . . .").
[127] Ex. 5. This policy is publicly available at the following website: http://tinyurl.com/mrh9wjx2. *See also Am. Libr. Ass'n, Inc.*, 539 U.S. at 206–07.
[128] *Supra*, 2–8.

Homeland Security designate UNT as a national cyber-defense-research center.[129]) Hacked messages could be used to coerce UNT students and employees. Pilfered location data could be used to track down critics of the CCP. And so on.

The risks are especially salient for government entities, which are "particularly visible targets" for cyberattacks according to the FBI.[130] Examples of such high-profile hacks include:

- *2013-14:* Hackers accessed the U.S. Office of Personnel Management's network and stole millions of records, including social security numbers.[131] Some affected individuals had their identities stolen and were subjected to financial fraud following the breach.[132]
- *March 2018:* Hackers hit nearly 4,000 computers belonging to the city of Atlanta.[133] The attack "disrupted" city operations and led to millions of dollars in losses for the city.[134]
- *May 2019:* Hackers seized around 10,000 Baltimore government computers, freezing certain city operations for two weeks.[135] One council member estimated that the city would have to spend $18 million to recover from this attack.[136]
- *August 2019:* A coordinated cyberattack crippled over 20 Texas entities for multiple days.[137]
- *May 2023:* A cyberattack took down Dallas city services, with some remaining offline for nearly two weeks.[138]
- *June 2023:* A cyberattack against Stephen F. Austin State University "caused serious

---

[129] *National Security Agency and Department of Homeland Security Name UNT a Center for Academic Excellence in Cyber Defense Research*, UNT (Mar. 19, 2015), https://tinyurl.com/28sa2jvp.
[130] *High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations*, FBI (Oct. 2, 2019), http://tinyurl.com/2axw4r53.
[131] *In re U.S. Off. of Pers. Mgmt. Data Sec. Breach Litig.*, 928 F.3d 42, 50–51 (D.C. Cir. 2019).
[132] *Id.* at 50.
[133] *Atlanta U.S. Attorney Charges Iranian Nationals for City of Atlanta Ransomware Attack*, DOJ (Dec. 5, 2018), http://tinyurl.com/2s39sht.
[134] *Id.*
[135] Emily Stewart, *Hackers have been Holding the City of Baltimore's Computers Hostage for 2 Weeks*, VOX (May 21, 2019), http://tinyurl.com/mr252vjv.
[136] *Ransomware Attack will Cost Baltimore City $18M, Councilmember Says*, CBS NEWS (May 30, 2019), http://tinyurl.com/hyy84ebr.
[137] *US Justice Department Announces Indictment Against REvil Ransomware Suspect Behind 2019 Ransomware Attack on Texas Municipalities*, TEX. DIR (Nov. 8, 2021), http://tinyurl.com/mrydap69; Manny Fernandez et al., *Ransomware Attack Hits 22 Texas Towns, Authorities Say*, N.Y. TIMES (Aug. 20, 2019), http://tinyurl.com/3k44xw3n.
[138] *City of Dallas Invests $4M in Cybersecurity After Ransomware Attack*, FOX 4 KDFW (June 29, 2023), http://tinyurl.com/4ysuw4yx; Tasha Tsiaperas, *Dallas City Sites Still Down After Cyberattack*, AXIOS (May 16, 2023), http://tinyurl.com/39dwdwy3.

disruptions" to the school for over a week.[139]

- *September 2023*: The Vietnamese government attempted to plant spyware known as "Predator" on the phones of federal employees and American journalists.[140]

Texas's partial ban is reasonably aimed at closing a vulnerability to its IT system. Texas was not constitutionally required to wait for the CCP to hack state agencies before acting to prevent this threat: "[T]he Government need not wait until havoc is wreaked to restrict access to a nonpublic forum."[141]

Also, Texas's partial ban leaves open ample alternative channels for communication, which further supports a reasonableness finding.[142] State employees and students can still use TikTok on personal devices that do not connect to state networks. That includes Professor Vickery. Despite claiming that her personal cellphone is a covered resource because she regularly connects it to state networks, Professor Vickery nowhere denies that she could stop using her personal cellphone that way—and rely instead on her university-issued computers for university-related work. She could also buy a personal laptop and use TikTok on it if she wanted to. Also notable, state employees and students can use practically any other social media application other than TikTok.

Finally, Texas was allowed to credit the wisdom and judgment of the many other governments—state, federal, and foreign—that have also restricted access to TikTok.[143] As the Fifth Circuit noted in *Gibson v. Collier:* "There is no reason why—as a matter of either common sense or constitutional law—one state cannot rely on the universally shared experiences and policy

---

[139] Kate McGee, *Stephen F. Austin State University Students Grow Anxious About Falling Behind as School Reels from Cyberattack Last Week*, TEX. TRIB. (June 21, 2023), http://tinyurl.com/57tjmjvy.
[140] Joseph Menn et al., *Vietnam Tried to Hack U.S. Officials, CNN with Posts on X, Probe Finds*, WASH. POST (Oct. 9, 2023), https://tinyurl.com/bddbtjm.
[141] *Cornelius*, 473 U.S. at 810.
[142] *See Perry Educ. Ass'n*, 460 U.S. at 53–54.
[143] *See Fla. Bar v. Went For It, Inc.*, 515 U.S. 618, 628 (1995) ("[W]e have permitted litigants to justify speech restrictions by reference to studies and anecdotes pertaining to different locales altogether, or even, in a case applying strict scrutiny, to *justify restrictions based solely on history, consensus, and simple common sense*.") (citations omitted) (emphasis added).

determinations of other states."[144] *Gibson's* statement has more force here. Our federal government and its allies—with their sophisticated intelligence resources and network of confidential sources—classify TikTok as a national security threat. A ruling against Defendants here amounts to a finding that these governments are *all* being unreasonable. Coalition presents no facts that plausibly support such a conclusion.

4. Texas's Partial TikTok Ban Would Survive Even the More Rigorous Scrutiny Applied to Designated and Traditional Public Forums.

Coalition's claims fail under even the higher scrutiny applied to designated and traditional public forums. Coalition does not allege that Texas's partial TikTok ban regulates speech based on viewpoint or content. Thus, the question is whether this ban is "narrowly tailored to serve a significant government interest[] and leave[s] open ample alternative channels of communication."[145]

Texas's ban serves at least three interests: privacy, security, and public safety. Binding precedent holds that these are significant government interests.[146] And the substantial consensus that TikTok poses a security threat, coupled with media reports showing the CCP's troubling ties to this company, satisfy the government's light burden on the "interest" issue.[147]

Moving on to the tailoring analysis, Texas's partial ban is narrowly tailored for the same

---

[144] 920 F.3d 212, 224 (5th Cir. 2019).

[145] *Perry Educ. Ass'n*, 460 U.S. at 45; *see also Mansky*, 138 S. Ct. at 1885.

[146] *Hous. Chron. Pub. Co. v. City of League City*, 488 F.3d 613, 622 (5th Cir. 2007) (public safety is a compelling interest); *United States v. Green*, 293 F.3d 855, 859 n.20 (5th Cir. 2002) (national security is a substantial interest); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 192 (5th Cir. 2000) (confidentiality of private communications is a substantial interest).

[147] *See, e.g.*, *City of Los Angeles v. Alameda Books, Inc.*, 535 U.S. 425, 438 (2002) ("[A] municipality may rely on any evidence that is reasonably believed to be relevant for demonstrating a connection between speech and a substantial, independent government interest.") (quotations omitted); *Went For It, Inc.*, 515 U.S. at 628 ("[W]e have permitted litigants to justify speech restrictions by reference to studies and anecdotes pertaining to different locales altogether, or even, in a case applying strict scrutiny, to justify restrictions based solely on history, consensus, and simple common sense.") (citations omitted); *Doe I v. Landry*, 909 F.3d 99, 109 (5th Cir. 2018) ("The evidentiary burden to support the governmental interest is light."); *id.* at 110 ("[W]e have allowed such regulations to be justified by evidence that may not have been presented to the enacting officials and was only produced at the time of trial.").

reasons it is "reasonable." As one court recently explained, limiting a security-related restriction to government devices is the "obvious alternative" to fully banning a Chinese-based application.[148] Texas did not violate the First Amendment when it adopted the "obvious alternative" here.

Reviewing *Ward v. Rock Against Racism*[149] helps confirm why Texas's partial ban is constitutional. There, New York City had regulated the volume of music at an amphitheater in Central Park to make sure performances were satisfactory while not intruding on the peace and quiet of nearby residents.[150] The main issue was excess noise at the amphitheater, and the city found that the problem was largely caused by the use of (1) inadequate sound equipment and (2) unskilled sound technicians.[151] The city passed guidelines that required performers to use high quality sound equipment and experienced sound technicians furnished by the city.[152] One performer, Rock Against Racism ("RAR"), wanted to "use its own sound equipment and technician, just as it had done in prior years."[153] RAR challenged the city's guidelines under the First Amendment.

The Second Circuit found in RAR's favor, believing the city's guidelines were not narrowly tailored as there were less intrusive means to achieve the city's goals.[154] The Supreme Court reversed. The Court found that a speech restriction need not be the least restrictive way to achieve the government's interests to satisfy intermediate scrutiny.[155] The Court found that the guideline's sound technician requirement was narrowly tailored to the city's interest in limiting volume, stating that,

---

[148] *U.S. WeChat Users All. v. Trump*, 488 F. Supp. 3d 912, 917, 927 (N.D. Cal. 2020).
[149] *Ward v. Rock Against Racism*, 491 U.S. 781 (1989).
[150] *Id.* at 784.
[151] *Id.* at 786.
[152] *Id.* at 787.
[153] *Id.*
[154] *Id.* at 797–98.
[155] *Id.* at 800 ("[A]s the means chosen are not substantially broader than necessary to achieve the government's interest, . . . the regulation will not be invalid simply because a court concludes that the government's interest could be adequately served by some less-speech-restrictive alternative.").

"[a]bsent this requirement, the city's interest would have been served less well."[156] The Court also noted that the Second Circuit's analysis "reflect[ed] nothing more than a disagreement" over how the city should achieve its desired goals and stated that the Second Circuit "erred in failing to defer to the city's reasonable determination" on this point.[157]

Ward also clarified the scope of an intermediate scrutiny inquiry. RAR wanted to focus the analysis on its specific situation. Under this view, the city's interest in promoting sufficient sound amplification for concertgoers would not be narrowly tailored as RAR's performances were historically "characterized by more than adequate sound amplification."[158]

Ward rejected this framing, finding that "the validity of the regulation depends on the relation it bears to the overall problem the government seeks to correct, not on the extent to which it furthers the government's interests in an individual case."[159] The Court continued: "Here, the regulation's effectiveness must be judged by considering all the varied groups that use the bandshell, and it is valid so long as the city could reasonably have determined that its interests overall would be served less effectively without the sound-amplification guideline than with it."[160]

Ward is instructive here. First, Texas's interests in privacy, security, and safety would be "served less well" absent the partial TikTok ban. Coalition does not appear to dispute that this ban makes it at least somewhat harder for the CCP to exploit its ability to access TikTok to the state's detriment. Even a minor reduction in risk would justify Texas's actions. And this Court should be hesitant to second-guess Texas's and the federal government's responses on the TikTok issue.[161] As

---

[156] *Id.*
[157] *Id.*
[158] *Id.* at 801.
[159] *Id.*
[160] *Id.*
[161] *See id.* at 800 (finding that the Second Circuit should have "defer[red] to the city's reasonable determination" that its interests would be best served by the guidelines); *United States v. Albertini*, 472 U.S. 675, 689 (1985) ("The validity of [content-neutral time, place, or manner] regulations does not

Coalition itself admits, a failure in Texas's security that leads to a CCP cyberattack would be "a catastrophic foreign relations problem" that would put our respective countries "on the brink of war."[162]

Second, Coalition argues that Texas's partial ban is unconstitutional as it does not carve out a few narrow exceptions for certain university professors.[163] *Ward* shows that intermediate scrutiny does not require this level of fine tuning. Again, a content-neutral regulation such as Texas's partial ban "need not be the least restrictive or least intrusive means" to achieve the state's interests to survive intermediate scrutiny.[164]

Third, Coalition wants to invalidate Texas's partial ban due to its impact on a small fraction of the Texas state workforce—here, only one identified UNT professor.[165] *Ward* shows that this Court's analysis must instead (1) focus "on the relation [Texas's partial ban] bears to the overall problem the government seeks to correct, not on the extent to which it furthers the government's interests in an individual case" and (2) judge the effectiveness of this ban "by considering all the varied groups" impacted by this policy.[166] Coalition did not show that Texas's partial ban is overbroad when considering the scope of the problem Texas faces: The state employs hundreds of thousands of

---

turn on a judge's agreement with the responsible decisionmaker concerning the most appropriate method for promoting significant government interests.").

[162] ECF 20-3, ¶ 38.

[163] *See generally* ECF 1.

[164] *Ward*, 401 U.S. at 799.

[165] *Cf.* Anderson Decl., ¶ 6 (noting that only six scanned UNT-issued devices out of 18,000 had TikTok installed).

[166] *Ward*, 401 U.S. at 801; *see also Albertini*, 472 U.S. at 688–89 ("Regulations that burden speech incidentally or control the time, place, and manner of expression, must be evaluated in terms of their general effect.") (citations omitted); *Moore v. Brown*, 868 F.3d 398, 404 (5th Cir. 2017) ("Moore argues that that the Defendants fail to demonstrate how banning his sketch board furthers their safety interest. But this argument improperly frames the inquiry: challenged rules must be evaluated in terms of their *general* effect.").

individuals,[167] each of whom is a potential vector for a CCP-sponsored cyberattack.[168]

Finally, *Ward* found the ample alternative channels requirement "easily met" as the city's guidelines "do[] not attempt to ban any particular manner or type of expression at a given place or time."[169] The same is true here: Texas's partial ban leaves users free to say anything they want on or about TikTok, and they can still access this platform through personal devices not connected to state networks. This includes university employees like Professor Vickery. In sum, there are no plausible grounds for finding that Texas's limited TikTok ban violates the First Amendment, regardless of the type of forum involved.

5. Coalition's Arguments do Not Change the Analysis Above.

(a) "*NTEU*" Scrutiny does Not Apply to Nonpublic Forums.

Coalition likens Texas's partial ban to a prior restraint on speech, and thus it asks this Court to apply a higher level of constitutional scrutiny known as "*NTEU*" scrutiny.[170] It missed that prior restraints *in nonpublic forums* are still subject only to a "reasonableness" review.[171] Thus, in *Freedom From Religion Foundation v. Abbott*, which involved a prior restraint in a nonpublic forum, the Fifth Circuit applied the lower "reasonableness" standard, as opposed to something resembling strict scrutiny.[172]

---

[167] *See Overview*, TEX. AUDITOR'S OFFICE, https://tinyurl.com/3beham52.

[168] *See* ECF 21, 28–29 (explaining how a cyberattacker could exploit access to one employee or device to infiltrate other devices or other parts of the state's network); *see also* Frkuska Decl., ¶ 6 (noting some of the difficulties with drafting a statewide policy that adequately protects all approximately 200 state agencies in Texas).

[169] *Ward*, 401 U.S. at 802.

[170] ECF 20, 10–24.

[171] *Perry v. McDonald*, 280 F.3d 159, 171 (2d Cir. 2001) ("Prior restraints in a nonpublic forum have been upheld as long as they were reasonable and viewpoint-neutral.") (citing *Cornelius*, 473 U.S. at 813); *Milwaukee Police Ass'n v. Jones*, 192 F.3d 742, 749 (7th Cir. 1999) ("[A] prior restraint on speech in a non-public forum at a school is constitutional if reasonably related to legitimate pedagogical goals. . . . [E]ven in cases of a prior restraint on speech, the context in which the restriction occurs can affect the level of scrutiny applied.").

[172] 955 F.3d 417, 429 (5th Cir. 2020); *see also Catholic Leadership Coal. of Tex. v. Reisman*, 764 F.3d 409, 438–39 (5th Cir. 2014) ("[J]udicial decisions analyzing prior restraints have applied different standards of review depending on the restraint at issue.").

The reasoning is simple. Nonpublic forums exist only when the government places limits in advance on what or where speech can occur on government property. Considering every such limit to be a "prior restraint" would eviscerate decades of Supreme Court precedent (1) distinguishing between public and nonpublic forums and (2) applying lighter scrutiny to the latter.[173]

For similar reasons, a content-neutral time, place, or manner regulation in a traditional or designated forum receives only intermediate scrutiny, not the more exacting scrutiny applied to other prior restraints. As the Supreme Court explained in *Thomas v. Chicago Park Dist.*, prior restraints on the subject matter of speech raise censorship concerns that warrant strict scrutiny.[174] "[B]ut [a] content-neutral time, place, and manner regulation of the use of a public forum" generally does not raise such concerns as it does not restrict "what a speaker might say."[175] Thus, such content-neutral regulations, even when considered a "prior restraint," still receive only intermediate scrutiny.[176] An exception applies if the regulation gives government officials "unduly broad discretion" in determining what speech is and is not allowed on the government property,[177] but Coalition does not suggest that this exception applies here.

Another problem for Coalition is this case involves *access*, not *speech*, and "[t]he right of access does not enjoy the broad protections offered to the right of free speech."[178] For instance, in *Seattle Times Co. v. Rhinehart*,[179] the Supreme Court assessed the constitutionality of a protective order "that

---

[173] *See, e.g.*, *Perry*, 280 F.3d at 171.
[174] 534 U.S. 316, 321–22 (2002).
[175] *Id.* at 322.
[176] *Forsyth Cnty., Ga. v. Nationalist Movement*, 505 U.S. 123, 130 (1992); *GEFT Outdoor, LLC v. Monroe Cnty., Indiana*, 62 F.4th 321, 327 (7th Cir. 2023) ("[P]rior restraints are constitutionally sound time, place, or manner restrictions as long as they are content neutral, are narrowly tailored to serve a significant government interest, leave open alternative avenues for speech, and do not put too much discretion in the hands of government officials."); *see also Boardley v. U.S. Dep't of Interior*, 615 F.3d 508, 516 (D.C. Cir. 2010); *Burk v. Augusta-Richmond Cnty.*, 365 F.3d 1247, 1264 (11th Cir. 2004).
[177] *Thomas*, 534 U.S. at 323.
[178] *Matter of Subpoena 2018R00776*, 947 F.3d 148, 155–56 (3d Cir. 2020).
[179] 467 U.S. 20 (1984).

both granted [a litigant] access to that information and placed restraints on the way in which the information might be used."[180] The Court noted that this restriction was not the "classic" type of prior restraint "that requires exacting First Amendment scrutiny."[181] The Court found that the protective order was constitutional, largely because the litigant was free to "disseminate the identical information covered by the protective order as long as the information is gained through means independent of the court's processes."[182] So too here. Coalition's members, and Professor Vickery, can access TikTok, conduct research on TikTok, and review scholarship on TikTok whenever they want, so long as they do so on anything other than the state's networks or devices. And the fact that they remain free to say *anything* they want on or about TikTok means that Texas's partial ban burdens First Amendment rights even less than the restriction upheld in *Seattle Times*.

(b) Coalition's "Interests" Analysis is Deeply Flawed.

Coalition applies the balancing test designed mainly for First Amendment retaliation claims in the government employment context.[183] This test is a bad fit here, as Texas's ban is not limited to employees (it bars *anyone* from accessing TikTok on state networks, such as university students).[184] The ban leaves state employees free to say anything they want on or about TikTok, in stark contrast to the normal First Amendment employment case where the government is retaliating against an employee for his or her speech on a particular issue.

Regardless, Coalition loses even if an employment-based First Amendment test applies. As explained above, Texas's partial TikTok ban survives the generally applicable forum analysis.[185] This means the ban *must* survive constitutional scrutiny under an employment-based test, as binding

[180] *Id.* at 32.
[181] *Id,* at 33.
[182] *Id.* at 34.
[183] *See* ECF 20, 10–23.
[184] *Id.* at 15–16.
[185] *Supra*, 13–25.

precedent shows that "[a] government entity has broader discretion to restrict speech when it acts in its role as employer."[186] Put differently, that a government workplace is implicated *lessens*, not *raises*, the government's burden in this context.[187] Thus, an employment-based analysis cannot save Coalition here.

What's more, Texas's asserted interests for its partial ban—public safety, privacy, and security[188]—fit comfortably within the First Amendment employment test. Any different conclusion would lead to absurd results. CIA and NSA employees could not be stopped from using potentially harmful software (like TikTok), as national security would no longer be a viable government interest in the employment context. U.S. Social Security Administration employees could not be barred from disclosing individuals' social security numbers to the world, as the federal government would be powerless to restrict employee speech due to privacy concerns, and so on.

Further, the Supreme Court has recognized the "effective functioning of the public employer's enterprise" as a viable government interest in the employment context.[189] This category is broad enough to encompass well-recognized interests such as the ones Texas asserts here.[190] Coalition's core argument on this point—that national security, public safety, and privacy are no longer valid government interests in the employment free speech context—borders on the absurd.

Coalition's argument on the "privacy" issue is particularly confusing. Coalition effectively contends that everyone's personal data has already been stolen, so governments should stop trying to

---

[186] *Garcetti v. Ceballos*, 547 U.S. 410, 418 (2006); *see also Waters v. Churchill*, 511 U.S. 661, 671–72 (1994) ("[W]e have always assumed that its premise is correct—that the government as employer indeed has far broader powers than does the government as sovereign.").
[187] *See supra*, 17–18.
[188] *Id.* at 21.
[189] *Rankin v. McPherson*, 483 U.S. 378, 388 (1987).
[190] *See, e.g.*, *United States v. Wallington*, 889 F.2d 573, 578–79 (5th Cir. 1989) (finding that "[p]reserving the confidentiality of government records and reports" is a valid government interest in the employment context).

prevent the theft of personal data.[191] Defendants have a different opinion: Governments should not raise the white flag and subject adult citizens, their children, and future generations to a lifetime of privacy invasions and data theft.

Equally puzzling, Coalition *admits* that Americans' personal data has "significant intelligence value" that can "easily" be exploited by "foreign adversaries."[192] If so, shouldn't governments try to stop the CCP, a foreign adversary, from nefariously accessing the "significant intelligence" data TikTok maintains on over a hundred million American users? One would think so, especially when this data includes users' passwords, secret messages, financial information, and anything else that could be grabbed via TikTok's unusual "keylogging" feature.[193]

The dangers from TikTok are real—the actions of many states and countries that have partially banned this application prove that point better than words ever could. While Coalition believes that *all* these governments are wrong and acting unreasonably, it didn't offer facts plausibly supporting this conclusion.

6. Schneier's Declaration does Not Meaningfully Impact this Litigation; if Anything, His Writings Hurt Coalition's Position.

Coalition leans heavily on a declaration from its cybersecurity expert, Bruce Schneier.[194] Yet Schneier's declaration and other writings ultimately show why Texas's partial TikTok ban is constitutional.

(a) All Parties Agree that the CCP's Ability to Exploit TikTok Poses a Significant Risk to the United States' Interests.

Per Schneier, TikTok and ByteDance are "shady" companies that "operate at the pleasure of

[191] *See* ECF 20, 20–22.
[192] *Id.* at 21.
[193] *See id.* at 20–22. Coalition does not claim that data such as this is already commercially available.
[194] *See* ECF 20-3.

the Chinese government."[195] A report he co-authored for the Hoover Institution (the "Hoover Report")—which he cites multiple times in his declaration[196]—clarifies the nature and scope of the threat at issue here.[197]

The Hoover Report found that a "foreign adversary like the Chinese government" could use user data to "discover highly granular information about particular individual[s] or group attributes."[198] This creates "significant risks" for the United States, as the CCP could use this data "for identity exploitation, influence, and control."[199] The Hoover Report identified ByteDance as having a particularly "immense data set" that could be exploited by the CCP.[200]

In the opening paragraph of its complaint, Coalition contends that Texas's TikTok ban is overbroad as it is not limited to "state employees who have access to especially sensitive information or locations."[201] Schneier's Hoover Report undercuts this point. Per this Report, even data belonging to individuals without access to classified information "can be collected and aggregated" in a way that creates "national security risks."[202] For instance, if an individual is "connected with" or "linked to" a person with sensitive information, the individual and his connected devices become "potential vectors for a malicious actor to gain access to sensitive data and systems."[203] The Hoover Report identified "email phishing" as a way a hacker could exploit access to one individual to gain access to another's

---

[195] *Banning TikTok*, SCHNEIER ON SECURITY (Feb. 27, 2023), https://tinyurl.com/4f4xh66p; *see also* ECF 20-3, ¶ 5 (in which Schneier admits that "Schneier on Security" is his blog).
[196] ECF 20-3, ¶¶ 5, 21, 24, 37, 44, 50.
[197] *See* Gary Corn, Jennifer Daskal, Jack Goldsmith, Chris Inglis, Paul Rosenzweig, Samm Sacks, Bruce Schneier, Alex Stamos & Vincent Stewart, *Chinese Technology Platforms Operating in the United States*, HOOVER INST. (the "Hoover Report"), *available at* https://tinyurl.com/2zvprv4y.
[198] *Id.* at 4.
[199] *Id.*
[200] *Id.* at 6.
[201] ECF 1, ¶ 1.
[202] *Hoover Report*, *supra* note 198, 5.
[203] *Id.*

confidential information.[204]

For another example, the data of an individual who "is not a valuable source or target . . . can be combined with others—thus becoming a data point that subsequently enables an actor to carry out better targeting [and] analysis."[205] Per the Report, this could "enable[] a foreign adversary like China to glean valuable information about patterns of behavior, interests, and predispositions that could in turn be used to inform future intelligence, cyber, and information operations."[206]

Schneier's Hoover Report noted other dangers stemming from the CCP's ability to exploit technology companies like TikTok. One risk is that "Chinese technology platforms potentially provide ways in which access to communications systems becomes an easy means to manipulate users."[207] The Report notes that the CCP is currently "conduct[ing] influence operations to gather strategic intelligence about U.S. policies and personnel [and] to acquire technology from industrial espionage targets."[208] The concern is the CCP could expand these influence operations to "target democratic institutions or sow panic in moments of crisis," which would "further implicat[e] national security."[209] Another risk is the CCP could "leverage access to networks and individual devices such as smartphones to conduct malicious cyber operations."[210] The Report found that "[t]his kind of sabotage can be uniquely damaging but difficult to detect."[211]

In sum, all parties agree that the CCP's ability to exploit Chinese-controlled technology platforms like TikTok presents a significant risk to United States' interests. And while Schneier calls a

---

[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.* at 6.
[208] *Id.*
[209] *Id.*
[210] *Id.*
[211] *Id.*

partial TikTok ban "ineffective,"[212] he really means that it is *not as effective* as more comprehensive measures. Put simply, Coalition does not meaningfully dispute that Texas's partial ban will at least make it harder for the CCP to access state networks, harvest state employees' data, or otherwise influence state employees' actions. This is all that is needed to survive a narrow tailoring analysis.[213]

(b) If Texas's Partial TikTok Ban is Unconstitutional, So Too is the Biden Administration's.

An overarching problem with Schneier's arguments against Texas's TikTok ban is that they apply equally to the Biden Administration's TikTok ban. Schneier claims that the federal ban "appear[s] to cover a narrower set of employees or contain important exceptions that are missing from the Texas ban."[214] This is false. The Biden Administration's ban "applies to *all* executive agencies."[215] Further, the federal ban covers the "use or presence" of TikTok on all "information technology," which is defined broadly enough to cover the use of TikTok on a personal device connected to federal networks.[216]

As to exceptions, those in the federal ban are limited only to "law enforcement activities, national security interests and activities, and security research,"[217] none of which would apply here. Also, the federal ban allows these exceptions only when the use of TikTok is "critical to [the agencies'] mission."[218] Coalition cannot claim that an exception is "mission critical" for members like Professor

---

[212] ECF 20-3, ¶ 16.
[213] *See supra*, 22–26.
[214] ECF 20-3, ¶ 14.
[215] *February 27th Memorandum*, *supra* note 37, at II (emphasis added).
[216] *Id.* at II–III (incorporating the term "information technology" as defined in 40 U.S.C. § 11101(6)); 40 U.S.C § 11101(6) (defining "information technology" to include "any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly").
[217] *February 27th Memorandum*, *supra* note 37, at IV.A.
[218] *Id.* at IV.A.

Vickery, who works for a university—not an intelligence agency—and who admits that Texas's ban leaves her at least *some* other options for researching and teaching about TikTok.[219]

(c) Texas is Not Required to Fix *All* Privacy Issues Before Acting to Stop the CCP from Exploiting its Access to TikTok.

Schneier claims that, instead of partially banning TikTok, Texas could have: (1) enacted comprehensive privacy legislation; (2) required TikTok to store Americans' data in the U.S.; (3) tried to mitigate the spread of disinformation; and (4) established evaluation and testing centers for TikTok.[220] Schneier's proposals would be wildly out of place in even the strictest constitutional scrutiny analysis.

Schneier acts as if Texas cannot stop the CCP from exploiting its access to TikTok unless the state fundamentally reforms the trillion-dollar enterprise of aggregating and mining personal data.[221] Our country would grind to a halt if federal and state governments could only fix one problem by solving all other associated issues. Of course, that is not how our Constitution works: "The First Amendment does not put a State to [an] all-or-nothing choice."[222]

Equally troubling, Schneier does not account for the obvious constitutional problems with his identified "solutions." For instance, he proposes that Texas "require TikTok and other platforms to disclose its contacts and connections with foreign governments."[223] This could raise First Amendment compelled speech issues.[224] And he says Texas could comprehensively test TikTok or otherwise

[219] *See* ECF 20-2, ¶¶ 53–56.
[220] ECF 20-3, ¶¶ 21, 44–47, 50.
[221] *See* Nicholas Confessore, *The Unlikely Activists Who Took On Silicon Valley—and Won*, N.Y. TIMES MAGAZINE (Aug. 14, 2018), https://tinyurl.com/y946nj6n.
[222] *Williams-Yulee v. Florida Bar*, 575 U.S. 433, 452 (2015).
[223] ECF 20-3, ¶ 47.
[224] *See, e.g.*, *Amawi v. Pflugerville Indep. Sch. Dist.*, 373 F. Supp. 3d 717, 754 (W.D. Tex. 2019), *vacated and remanded sub nom. Amawi v. Paxton*, 956 F.3d 816 (5th Cir. 2020).

require it to store data in the U.S.[225] This is problematic in part due to the Foreign Commerce Clause.[226]

Also, Schneier never explains how much time, money, and manpower his comprehensive proposals would cost Texas. And he admitted elsewhere that one of his proposals—storing TikTok's data in the U.S.—wouldn't even work. As the Hoover Report found, the national security concerns associated with the CCP's access to user data apply even when that "data [is] stored outside of China's borders."[227]

If Schneier's alternatives were so obvious and easy, state and federal governments would have adopted them a long time ago.[228] But the devil is in the details. And there are a whole lot of "devils" in Schneier's proposals.

(d) Schneier's Narrower Proposals are Legally Irrelevant.

Schneier proposes that Texas (1) limit its ban to employees with especially sensitive information or (2) allow access to TikTok on dedicated devices or networks not connected to the state agency at large.[229] Yet the Hoover Report found that limiting a ban to employees with sensitive information would not work, and it noted some ways a foreign adversary could exploit such a vulnerability.[230] Also, this solution is not practical here. This is because most UNT employees have access to sensitive data in at least some way—such as information protected by the Family Educational

---

[225] ECF 20-3, ¶¶ 46, 50.

[226] *See Piazza's Seafood World, LLC v. Odom*, 448 F.3d 744, 750 (5th Cir. 2006) (explaining that, under the Foreign Commerce Clause, "nondiscriminatory state regulations affecting foreign commerce are invalid if they (1) create a substantial risk of conflicts with foreign governments; or (2) undermine the ability of the federal government to 'speak with one voice' in regulating commercial affairs with foreign states") (quotations omitted).

[227] *Hoover Report*, *supra* note 198, 2–3.

[228] The Biden Administration is starting to require TikTok to store user data in the United States. Yet it still believes that a partial ban on federal employees' use of TikTok is needed on top of this option. And recent reports have found security problems with these local data centers. *See* Emily Baker-White, *Security Failures at TikTok's Virginia Data Centers: Unescorted Visitors, Mystery Flash Drives and Illicit Crypto Mining*, FORBES (Apr. 21, 2023), https://tinyurl.com/bdhxbwuw.

[229] ECF 20-3, ¶¶ 48–49.

[230] *Supra*, 30–33.

Rights and Privacy Act.[231] As to Schneier's "dedicated device" proposal, state employees would still be giving their personal information to TikTok, and the Hoover Report found that the Chinese government could exploit such data for "future intelligence, cyber, and information operations."[232]

More importantly, Schneier's alternatives are legally relevant. Even if intermediate scrutiny applies (as opposed to a "reasonableness" standard), *Ward* shows that Texas's partial ban is not invalid just because there are hypothetical less restrictive means to achieve the state's interests.[233] *Ward* also rejected Schneier's narrow framing of the issue—as he focuses on how the ban impacts a sliver of state employees, instead of on the "overall problem" Texas is trying to solve.[234]

For the reasons above, Coalition is not likely to succeed on the merits. As shown below, the remaining preliminary injunction factors also favor Defendants.

II. The Remaining Preliminary Injunction Factors are in Defendants' Favor.

The harm to Coalition's members is minor, especially when compared to the risk of harm associated with a wrongful injunction. Coalition identified only one member, UNT professor Vickery, whose scholarship about TikTok is limited by Texas's partial ban. And even this one person admits that she can access TikTok and teach about this platform in other ways.[235] Further, a wrongful injunction could be catastrophic. It would open a vulnerability in Texas's network that the CCP could exploit to wreak havoc on the state's operations and employees, as has happened in the past due to less sophisticated cyberattacks.[236]

Further, the status quo favors Defendants. Coalition's members have been operating under a partial TikTok ban for over nine months—ever since Governor Abbott's December 7. 2022. An

[231] *See* Anderson Decl., ¶¶ 16–18.
[232] *Hoover Report*, *supra* note 198, 5.
[233] *Supra*, 23–26.
[234] *Id.*
[235] ECF 20-2, ¶¶ 53–56.
[236] *See supra*, 20–21.

injunction is disfavored as it would disrupt this status quo.[237]

Finally, Coalition unduly delayed in seeking emergency relief. This Court has found that "'[d]elay in seeking a remedy is an important factor bearing on the need for a preliminary injunction,'" particularly when the moving party provides no good excuse for its delay.[238] Further, this Court has held that unjustified delays of five or six months weigh against issuing a preliminary injunction.[239] Coalition delayed longer than this before seeking a preliminary injunction. And it has not, and seemingly cannot, establish good cause for waiting so long to seek this injunction. This alone supports a denial of Coalition's motion for a preliminary injunction.

CONCLUSION

For the reasons above, this Court should deny Coalition's motion for a preliminary injunction.

Date: October 23, 2023

Respectfully Submitted.

KEN PAXTON
Attorney General of Texas

BRENT WEBSTER
First Assistant Attorney General

GRANT DORFMAN
Deputy First Assistant Attorney General

JAMES LLYOD
Deputy Attorney General for Civil Litigation

KIMBERLY GDULA
Acting Division Chief, General Litigation Division

/s/ Todd Dickerson
TODD A. DICKERSON

---

[237] *See Feds for Med. Freedom*, 63 F.4th at 389; *Martinez*, 544 F.2d at 1243.
[238] *Luckenbach Tex., Inc. v. Skloss*, No. 1:21-CV-871-RP, 2022 WL 5568437, at *4 (W.D. Tex. July 8, 2022) (quoting *Massimo Motor Sports LLC v. Shandong Odes Indus. Co.*, No. 3:21-CV-02180-X, 2021 WL 6135455, at *2 (N.D. Tex. Dec. 28, 2021)).
[239] *See Digerati Distribution & Marketing, LLC v. Sarl*, No. 1:22-CV-01302-DII, 2023 WL 5687040, at *3 (W.D. Tex. Aug. 2, 2023); *Career Colleges & Sch. of Tex. v. United States Dep't of Educ.*, No. 1:23-CV-433-RP, 2023 WL 4291992, at *5 (W.D. Tex. June 30, 2023).

Attorney-in-Charge
Texas Bar No. 24118368
Todd.Dickerson@oag.texas.gov
Assistant Attorney General
Office of the Attorney General
P.O. Box 12548-Capitol Station
Austin, Texas 78711-2548
(512) 463-2120
FAX: (512) 320-0667
COUNSEL FOR DEFENDANTS

CERTIFICATE OF SERVICE

I hereby certify that on October 23, 2023, a true and correct copy of the foregoing instrument has been served electronically through the electronic-filing manager to:

Peter B. Steffensen
SMU Dedman School of Law
First Amendment Clinic
P.O. Box 750116
Dallas, TX 75275
(214) 768-4077
psteffensen@smu.edu

Jameel Jaffer*
Ramya Krishnan*
Stacy Livingston*
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
(646) 745-8500
jameel.jaffer@knightcolumbia.org
COUNSEL FOR PLAINTIFF

/s/ Todd Dickerson